I claim:

1. A computer program product for using biometrics on pervasive devices for mobile identification, said computer program product embodied on a medium readable by said pervasive device and comprising:

programmable code means for capturing biometric data of a third party using a biometric input reader which is attached to or incorporated within a mobile pervasive device; and

programmable code means for identifying said third party using said captured biometric data by comparing said captured biometric data to previously-stored biometric data.

2. The computer program product according to Claim 1, further comprising:

programmable code means for transmitting said captured biometric data from said mobile pervasive device to a remote server;

programmable code means for retrieving, by said remote server, information from a repository using said transmitted biometric data; and

programmable code means for returning said retrieved information to said mobile pervasive device.

3. The computer program product according to Claim 2, wherein said retrieved information comprises a photograph of a party to whom said biometric data corresponds.

4. The computer program product according to Claim 2, wherein said retrieved information comprises access rights of a party to whom said biometric data corresponds.

5. The computer program product according to Claim 2, wherein said retrieved information comprises protected information not locally accessible to said mobile pervasive device.

6. The computer program product according to Claim 2 or Claim 5, further comprising:

programmable code means for filtering, by said remote server, said retrieved information based upon a determined identity of said third party; and

wherein said returned retrieved information is said filtered retrieved information.

7. The computer program product according to Claim 1, wherein said mobile pervasive device further comprises a locally-stored repository containing said previously-stored biometric data, and wherein said programmable code means for identifying compares, by said mobile pervasive device, said captured biometric data to said previously-stored biometric data in said locally-stored repository.

8. The computer program product according to Claim 1, wherein said computer program product is used to enable on-demand creation of a secure meeting site by repeating operation of said programmable code means for capturing and said programmable code means for identifying for each of a plurality of meeting attendees.

9. The computer program product according to Claim 1, wherein said computer program product is used to exchange a trusted message by performing operation of said programmable

code means for capturing and said programmable code means for identifying wherein said third party is a potential recipient of said trusted message.

10. A system for using biometrics on pervasive devices for mobile identification, said system comprising:

a mobile pervasive device;

a biometric input reader attached to or incorporated within said mobile pervasive device;

means for capturing biometric data of a third party using said biometric input reader; and

means for identifying said third party using said captured biometric data by comparing said captured biometric data to previously-stored biometric data.

11. The system according to Claim 10, further comprising:

means for transmitting said captured biometric data from said mobile pervasive device to a remote server;

means for retrieving, by said remote server, information from a repository using said transmitted biometric data; and

means for returning said retrieved information to said mobile pervasive device.

12. The system according to Claim 11, wherein said retrieved information comprises a photograph of a party to whom said biometric data corresponds.

13. The system according to Claim 11, wherein said retrieved information comprises access rights of a party to whom said biometric data corresponds.

14. The system according to Claim 11, wherein said retrieved information comprises protected information not locally accessible to said mobile pervasive device.

15. The system according to Claim 11 or Claim 14, further comprising:

means for filtering, by said remote server, said retrieved information based upon a determined identity of said third party; and

wherein said returned retrieved information is said filtered retrieved information.

16. The system according to Claim 10, wherein said mobile pervasive device further comprises a locally-stored repository containing said previously-stored biometric data, and wherein said means for identifying compares, by said mobile pervasive device, said captured biometric data to said previously-stored biometric data in said locally-stored repository.

17. The system according to Claim 10, wherein said system is used to enable on-demand creation of a secure meeting site by repeating operation of said means for capturing and said means for identifying for each of a plurality of meeting attendees.

18. The system according to Claim 10, wherein said system is used to exchange a trusted message by performing operation of said means for capturing and said means for identifying wherein said third party is a potential recipient of said trusted message.

19. A method for using biometrics on pervasive devices for mobile identification, said method comprising the steps of:

capturing biometric data of a third party using a biometric input reader attached to or incorporated within a mobile pervasive device; and

identifying said third party using said captured biometric data by comparing said captured biometric data to previously-stored biometric data.

20. The method according to Claim 19, further comprising the steps of:

transmitting said captured biometric data from said mobile pervasive device to a remote server;

retrieving, by said remote server, information from a repository using said transmitted biometric data; and

returning said retrieved information to said mobile pervasive device.

21. The method according to Claim 20, wherein said retrieved information comprises a photograph of a party to whom said biometric data corresponds.

22. The method according to Claim 20, wherein said retrieved information comprises access rights of a party to whom said biometric data corresponds.

23. The method according to Claim 20, wherein said retrieved information comprises protected information not locally accessible to said mobile pervasive device.

24. The method according to Claim 20 or Claim 23, further comprising the step of:

filtering, by said remote server, said retrieved information based upon a determined identity of said third party; and

wherein said returned retrieved information is said filtered retrieved information.

25. The method according to Claim 19, wherein said mobile pervasive device further comprises a locally-stored repository containing said previously-stored biometric data, and wherein said identifying step compares, by said mobile pervasive device, said captured biometric data to said previously-stored biometric data in said locally-stored repository.

26. The method according to Claim 19, wherein said method is used to enable on-demand creation of a secure meeting site by repeating operation of said capturing step and said identifying step for each of a plurality of meeting attendees.

27. The method according to Claim 19, wherein said method is used to exchange a trusted message by performing operation of said capturing step and said identifying step wherein said third party is a potential recipient of said trusted message.